Paving the path to Secure Data Access with ***Safe-T RSAccess***

Recent researches show that six out of ten organizations around the globe have suffered at least one Cyber-attack incident on their networks, applications, websites, critical infrastructures, mobile, etc.

The common practice in organizations is to deploy defense layers acting as "walls" and "gates" protecting from intrusions to their internal networks. These defense layers include DMZ (demilitarized zone, also known as "perimeter") network segments and layers of firewalls.
However, the rise in number of cyber-attacks and data breached, shows us that the current network security paradigm is flawed.

DMZ network segments are deployed not only as defense layers but also in order to provide customers, partners and suppliers with controlled access to corporate data. As more and more sensitive data from the internal network is duplicated in the DMZ, this perimeter network designed to be a buffer zone has become a prime target for hackers, providing IT departments with the following challenges:

Risk of Sensitive Data Breach - the DMZ is now a hub of external facing services containing large amounts of sensitive data and personally identifiable information resulting in greater risk of data breaches.

Preventing Hacking into the Internal Network from the DMZ - most front-end servers located in the DMZ communicate with servers within the LAN through an incoming port in the firewall, which hackers can utilize to launch attacks into the internal network In addition such servers are accessible from the Internet and can be compromised by hackers, providing a second means of attacking the internal network.

Increased Capital Costs - the DMZ network configuration also imposes a costly burden on the enterprise's capital expenses requiring additional hardware and software licenses as a result of duplicating sensitive data in the DMZ.

Higher Operational Costs - This additional hosting and synchronization of duplicated data between the LAN and DMZ requires a complex layer of data and network operations which can be complicated.

It is clear then, that a paradigm change is needed in order to overcome the challenges of today's network security practices and effectively combat cyber-attacks.

Safe-T RSAccess – Disruptive Secure Data Access

RSAccess is a disruptive and breakthrough secure reverse-access solution that is designed to overcome the challenges of today's DMZ networks and network segmentation, prevent criminal application access, application hacking, and protect classified networks within the enterprise infrastructure.

With RSAccess organizations start their journey to complete elimination of the DMZ, close incoming ports in the firewall, and eliminate sensitive data and application servers from the DMZ while gaining immediate costs savings.

Safe-T's RSAccess is a dual node patented technology, which removes the need to open any ports within a firewall, while allowing secured network access between networks (through the firewall).

RSAccess Secure Front-End solution is a two tier deployment:

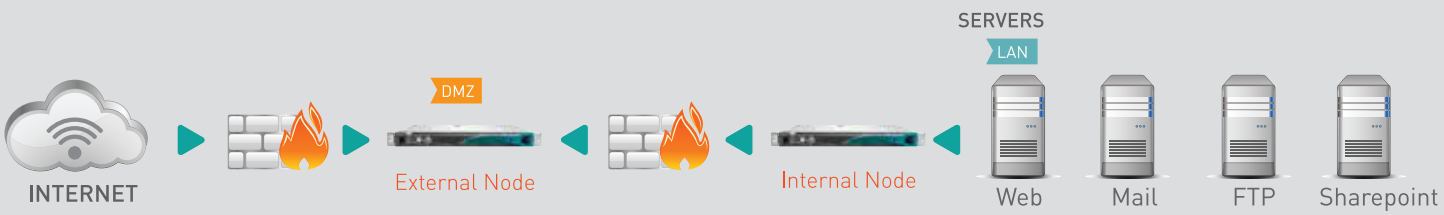
External RSAccess Node –
installed in the DMZ / external / non-secured segment

Internal RSAccess Node –
installed in the internal / secured segment

The role of the external RSAccess node is to act as a front-end to all services published within the DMZ. It operates without the need to open any ports within the external firewall and ensures that only legitimate session data can pass through into the LAN.

The role of the internal RSAccess node it to pull the session data into the LAN from the external RSAccess node, scan it using various application level security techniques, and then pass it to the destination application server.

> *"With RSAccess we were able to eliminate some of our web front-end servers in the DMZ, which resulted in a reduction of files storage in the DMZ, a cost reduction of applications servers and licenses and also worry-free secure collaboration with outside parties. Safe-T's innovative solution has improved both our IT security and efficiency."*
>
> ***Yuval Illuz,***
> ***Head of Global Infrastructure and IT Operations at ECI Telecom***



Eliminating the DMZ and Cyber Security Threats

By deploying Safe-T's patented RSAccess in the network, IT and application teams can fight off Hackers before they reach the perimeter, eliminating sensitive data and application servers from the DMZ, protecting their firewalls from attacks, all in a simple and cost-effective deployment. Gaining the following benefits in the process -

- ***Simplify network and DMZ architecture***
- ***Protect firewalls and networks from attacks***
- ***Eliminate sensitive data from DMZ, preventing compromising of***
- ***sensitive data***
- ***Improve data security by closing firewall ports that are constantly exploited by external hackers***
- ***Gain immediate costs savings by eliminating duplicated application licenses and hardware costs***
- ***Achieve increased operational efficiency by reducing constant data synchronization***
- ***Shorten the timeframe for regulation compliance***

Robust Deployment Scenarios

RSAccess's robust technology provides benefits in various deployment scenarios:

Secure Access Gateway for the Zero Trust Network
RSAccess improves the foundation of the Zero Trust Network design, by allowing secure reverse-access to Zero Trust Network MCAP segments, making it an even more secure and revolutionary design.

DMZ-as-a-Service Cloud
Secure reverse-access to entire organizations' data centers with a one-of-a-kind cloud security service. This solution enables complete masking of the organization's true location and architecture from external users and attackers.

Secure Application Front-end
Allows secure reverse-access to any application without opening any ports in the firewall, by deploying RSAccess as part of the application by an organization or software vendor (in the form of an OEM) in the DMZ.

RSAccess Features

- *Dual node patented solution*
- *Unidirectional application aware traffic flow*
- *No need to open incoming ports in the firewall*
- *IPSec tunnel between both nodes*
- *SSL offloading on internal node*
- *Block application, network and firewall based attacks*
- *On premise or cloud deployment*

SAFE-T
Smart Security Made Simple.

About Safe-T

Safe-T Data is a provider of data security solutions for a wide range of industries, including: financial, healthcare and manufacturing organizations.

Safe-T Data's Safe-T Box is a Secure Data Exchange Broker solution, which enables organizations enables organizations to broker, control and secure data exchange of any type and size between people, applications, cloud solutions, and businesses. It is designed to rapidly add security and control across a wide variety of data exchange Patterns for enterprises of all types including to and from the Cloud.

Safe-T's RSAccess Secure Data Access solution is disruptive and breakthrough secure reverse-access solution that is designed to overcome the challenges of today's DMZ networks and network segmentation, prevent criminal application access, application hacking, and protect classified networks within the enterprise infrastructure. Safe-T Data's secure front-end solution eliminates the need to store sensitive data in the DMZ, thereby reducing exposure to data breaches.

With offices in North America, Europe, and Israel, Safe-T Data secures millions of files and emails every day. For more information, visit **www.safe-t.com**.

© 2015 Safe-T Data Ltd. All Rights Reserved. Safe-T and all other Safe-T product and service names are registered trademarks of Safe-T Data in the U.S. and other countries. All other trademarks and names are the property of their respective owners